Self-Hosted Cryptocurrency Wallets Face New Privacy Hurdles

By **Justin Steffen and Guillermo Christensen** (January 5, 2021)

Justin Steffen

Guillermo Christensen

Bitcoin prices are rising, and the crypto bulls are back to touting crypto's superiority over more archaic forms of currency. Two recent developments, however, highlight that despite digital currency's potential, there are still regulatory and technical roadblocks to protecting financial privacy while using cryptocurrencies.

As in other areas of the digital economy, therefore, digital currency owners must closely consider how — and with whom — they choose to transact.

Digital Currencies and Self-Hosted Wallets

Cryptocurrencies, like bitcoin, frequently use public and private key cryptography. Users have both a public address and a private key. Anyone can send you cryptocurrency, so long as they know your public address. One, however, needs their private key to control and send their cryptocurrency.

Many use the analogy of a P.O. Box or a locked mailbox. Anyone can send you a letter, and anyone can deposit it into your mailbox. But to access your own mail, you need the key.

An individual's private key can take myriad forms, but traditionally it is a long series of alphanumeric characters. Like the mailbox analogy, private keys are incredibly valuable. If you lose the private key, you cannot access your cryptocurrency.

Conversely, if you give someone else your private key, they can take your cryptocurrency. As a result, how you store your private keys — sometimes referred to as "hodling"[1] — is critically important.

There are many ways to store a private key. Individuals, for instance, may choose to:

- Keep the keys on a hardware wallet — a storage device, like a USB drive, which can be purchased from a variety of companies, including Ledger SAS;
- Print the private key on a paper wallet, often in the form of a QR code; or
- Entrust the keys to a third party, often a cryptocurrency exchange or wallet service, who can store the keys in their own software wallet.

The first two options are often referred to as a form of "self-custody" or one that uses "self-hosted wallets." In comparison, when a third party is utilized, the storage device is often generically referred to as a "hosted wallet."

As in other financial transactions, when individuals utilize a third party, that third party has records and information relating to or revealing the individual's cryptocurrency holdings, which may become the subject of a government subpoena or other legal process.

Moreover, cybercriminals have targeted the third-party exchanges and wallet services that store their customer's keys. In 2018, for example, hackers absconded with $534 million of cryptocurrency from Japanese exchange Coincheck Inc.

Given the risks involved with trusting a third party, a number of industry insiders advocate that self-hosted wallets are preferable. Indeed, some proudly espouse the mantra "not your keys, not your crypto" to indicate that if you allow a third party to hold your private keys, you have no guarantee that you own or can control your digital currency.

In December 2020, two noteworthy developments revealed, however, that even self-hosted wallets may prove to be imperfect options, subject to both surveillance and attack.

FinCEN's Proposed Rule Concerning Self-Hosted Wallets and the Ledger Hack

On Dec. 18, the Financial Crimes Enforcement Network proposed new rules "aimed at closing anti-money laundering regulatory gaps for certain convertible virtual currency and digital asset transactions."[2] The new rules concern self-hosted cryptocurrency wallets.

Under the proposed rule, transactions involving self-hosted wallets would be subject to increased scrutiny. In particular, the rule envisions enhanced know-your-customer requirements for withdrawals of $3,000 or more to self-hosted wallets.

In addition, for transactions larger than $10,000, the rule requires money services business — those exchanges and wallet services who hold their customers' private keys — to obtain and file information pertaining to the customer and the counterparty, including the names and physical addresses of both parties.

Now, to transfer cryptocurrency from a hosted wallet to one's own self-hosted wallet, exchanges will be forced to procure and customers forced to provide additional information.

Then, on Dec. 20, hackers published personal information, including emails, physical addresses and phone numbers for over 270,000 Ledger customers. Ledger is a popular manufacturer of hardware wallets. The leak stems from a June data incident, that Ledger first disclosed in July.

Though the leak did not cause the loss of individuals' private keys, Ledger customers reported receiving threatening messages to their personal emails, demanding payment to be left alone.

The Future of Self-Hosted Wallets and Preserving Financial Privacy in the Cryptoverse

While many industry insiders were quick to provide detailed analyses of the FinCEN proposed rule — and its unusually short comment period of 15 days — the proposed rule combined with the Ledger leak should be particularly troubling for privacy and data security professionals.

The Ledger leak, like the myriad exchange incidents of prior years, is a further reminder that any third party, even tech-focused service providers, is vulnerable to attack. The more third parties that have your information, or your keys, the more targets exist for criminals to obtain and exploit that information.

The proposed FinCEN rule provides another potential point of compromise — the U.S. government. If FinCEN's self-hosted wallet rule is passed, exchanges and wallet services will be obligated to provide even more information regarding customers' holdings. This would be an even bigger honeypot for hackers.

Records maintained by FinCEN have been leaked in the past. In the fall of 2020, reporters obtained 2,100 suspicious activity report, believed to have been assembled during congressional attempts to investigate Russia's efforts to interfere with the 2016 election.[3]

Given these developments, hodlers will need to reevaluate how they store their cryptocurrency. To protect your keys or even your information from being reported or disclosed, individuals will first have to consider whether they use an exchange to obtain their cryptocurrency and in what quantities.

While it is possible to still move small amounts to or from a self-hosted wallet, the process may become more tedious. Individuals must understand that large transactions may be memorialized and shared with FinCEN. Then, hodlers should diligence those third parties whose goods and services they will use. To do so, consider the hallmarks of a company with strong data security practices and protections.

For example, where possible, look for service providers that open themselves up to third-party outside audits of their security practices and post general results of such evaluations. Another best practice is to see frequent patching and updates by the service provider of their systems: An infrequent record of updates should be viewed skeptically; no system exists without bugs.

Lastly, basic security measures, such as multifactor authentication, preferably implemented using hardware keys or app-based tokens are a must.

Going forward, regardless of how you store your digital assets, these recent developments demonstrate that you can control your own keys, but you cannot always control who knows how you hodl. Plan accordingly.

Justin C. Steffen is a partner at Ice Miller LLP.

Guillermo Christensen is a partner at the firm and a member of the Law360 Cybersecurity & Privacy Editorial Advisory Board.

[1] One who "hodls" buys and holds their crypto, rather than selling it. The term "hodl" is actually a typographical error from an early trader's bitcoin forum post that evolved into a meme.

[2] https://home.treasury.gov/news/press-releases/sm1216.

[3] https://www.brookings.edu/blog/up-front/2020/09/25/what-the-fincen-leaks-reveal-about-the-ongoing-war-on-dirty-money/.